Windcave

Merchant Operating Guide

Version 2.1

Copyright

Proprietary Notice

This document is uncontrolled when printed

Windcave

Document Revision Information and Amendments

All amendments are to be identified and the manual updated, noting the amendment on this amendment page.

Version	Date	Section	Revision Information	Amended by
0.1	2022/12/13	All	Migrated to new document format	NW
0.2	2023/01/14	All	Document updates	NW
0.3	2023/01/24	All	Updated imaging and content format	NW
0.4	2023/01/31	4	Added DCC information section	NW
0.5	2023/02/08	9	Updated PCI DSS Compliance information	NW
0.6	2023/02/21	2, 3, 4	Updated information / Added Surcharging	NW
1.0	2023/03/13	All	Release version	NW
1.1	2023/07/13	3	Added Connectivity information	NW
2.0	2023/08/23	5 13	Updated guidance for surcharging AMEX Cardholders in Australia and New Zealand Added section on AMEX	NW
2.0	2024/08/09	2	Updated guidance for Merchant Service Fees and Merchant Service Pricing Models	AS
2.1	2025/01/23	4.1.4, 11.1.3, 11.2.2	Updated Refunds section Updated PCI DSS compliance reporting Updated to reflect the change from GBPP to VIRP	SC

Related Documents

Document Title	Link/Location
Connectivity details	https://www.windcave.com/connectivity-about
Payline information	https://www.windcave.com/merchant-ecommerce-payline
Paylink information	https://www.windcave.com/developer-e-commerce-paylink
Rest API and its offerings	https://www.windcave.com/developer-e-commerce-api-rest
Visa PCI DSS Compliance	https://www.visa.co.nz/support/small-business/security-compliance.html
MasterCard site data protection	https://www.mastercard.com/global/en/business/overview/safety-and-security/security-recommendations/site-data-protection-PCI.html
American Express Data Security Requirements	http://www.americanexpress.com/dsr
List of PCI DSS approved QSA	https://listings.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors
List of PCI DSS Approved Scanning Vendors (ASV)	https://listings.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors
PCI compliance and reporting requirements	https://www.pcisecuritystandards.org
Visa Integrity Risk Program (VIRP)	https://corporate.visa.com/content/dam/VCOM/corporate/visa-perspectives/documents/protecting-the-integrity-of-the-visa-network.pdf
MasterCard Business Risk Assessment & Mitigation Program (BRAM)	https://www.mastercard.us/en-us/vision/who-we-are/terms-of-use/anti-piracy-policy.html#:~:text=The%20Anti-Piracy%20Policy%20supports%20and%20is,to%20the%20Mastercard%20network%20any%20transaction&text=The%20Anti-Piracy%20Policy%20supports,Mastercard%20network%20any%20transaction&text=Policy%20supports%20and%20is,to%20the%20Mastercard%20network
American Express Merchant Operating Guide	https://icm.aexp-static.com/content/dam/gms/en_us/optblue/us-mog.pdf

Contents

1 Overview 5
2 Understanding Merchant Services 6
2.1 Settlement 6
2.2 Merchant Statement 6
2.3 Merchant Service Fees (MSF) 6
3 Connectivity 8
4 Transaction Processing 8
4.1 Card Present (CP) 8
4.1.1 Contactless 9
4.1.2 Standalone Payment Solution 9
4.1.3 Card Validation 9
4.1.4 Refunds 10
4.1.5 Receipts 10
4.1.6 Fall-Back 10
4.1.7 Terminal Message Guide 11
4.1.7.1 Error Messages 11
4.2 Card Not Present Transactions (CNP) 12
4.2.1 E-Commerce Transactions 12
4.2.1.1 Windcave Hosted 12
4.2.1.2 Merchant Hosted 13
4.2.1.3 Recurring and Tokenization 14
4.2.1.4 Batch 15
4.2.1.5 3DS 15
4.2.2 MOTO (Mail Order/Telephone Order) 15
4.2.3 Processing a Refund 16
5 Surcharging 16
6 Dynamic Currency Conversion (DCC) 17
6.1 DCC Transaction Flow 17
6.2 Merchant Requirements 17
6.3 Best Practices 18
7 Offline Processing 18
8 Authorization 20
8.1 Card Present (CP) 20
8.2 Card Not Present (CNP) 20
9 Transactional Fraud Prevention 21
9.1 Card Not Present Fraud 21
9.2 Card Present Fraud 22

9.3 Transaction Fraud 23
9.4 Employee Fraud 23
10 Chargebacks 24
10.1 Common Chargebacks and Mitigation 25
11 Business Protection 27
11.1 PCI DSS 27
11.1.1 PCI DSS Requirements 27
11.1.2 Protection 28
11.1.3 PCI DSS Compliance Reporting 28
11.1.4 Obligation 29
11.2 Brand and Business Risk 29
11.2.1 Unacceptable businesses 29
11.2.2 BRAM and VIRP 30
11.3 Terminal Tampering 30
12 Support and Troubleshooting 31
12.1 Terminal not working 31
12.2 Cards Failing 31
13 American Express 33
13.1 American Express Merchant Operating Guide 33
13.2 Merchant Information 33
13.3 American Express Brand 33
13.4 Refund Policies 33
13.5 Limitation of Liability 34
13.6 Other 34
14 FAQ's 34
14.1 General FAQ's 34
14.2 Hosted Payment Page (HHP) 34
14.3 3D Secure Authentication 35
14.4 Batch Processor 35
14.5 Acquiring 35
14.6 Troubleshooting 35
15 Document Control Procedure 36

1 Overview

The Merchant Operating Guide will help you become familiar with the operation of your Merchant Facilities and the acceptance of payment scheme such as Visa, MasterCard, American Express and UnionPay Credit and Debit cards.

This guide forms part of your agreement with Windcave for Merchant facilities and may be varies or replaced by Windcave as required.

A clear understanding of your responsibilities as specified in this guide and in your Merchant Services Agreement will help avoid any misunderstands or disputes.

How to Contact Us

Phone Enquiries:

New Zealand
Freephone: 0800 PAYMENT (729 6368)
Or
+64 9 309 4693

Australia
Freephone: 1 800 006 254
Or
+61 2 8268 7700

UK & Europe
+44 2037523340

USA & Canada
+1 213 378 1190

Email Enquiries:

Windcave Acquiring team:
Acquiring@windcave.com

2 Understanding Merchant Services

Windcave facilitates seamless ecommerce, retail, and unattended transactions for customers around the world. Certified with all major credit card schemes and PCS DSS compliant, we provide innovative end-to-end payment solutions ensuring your transactions are safe, smooth, and secure.

Understanding the Merchant Services Windcave provides includes understanding your responsibilities. This includes:

- Follow the instructions in this guide
- Only process transaction types approved for you to process. These are detailed in the signature section of your merchant service agreement
- Check your statement regularly to ensure that your monthly Merchant Service Fee is correct
- Accept and validate all nominated cards presented for payment
- Ensure that the cardholder authorises all Credit Card transactions by using a PIN or signature, unless the transaction is by mail order, telephone order, via the internet or is a contactless transaction of $80.00 or less
- Don't split the cost of a single transaction between two or more sales receipts using a single cardholder account to avoid authorisation limits
- Don't give cash out with Credit Card transactions (including refunds)
- Don't impose a minimum or maximum amount on Credit or Debit card transactions
- Retain paper or electronic records of all transactions for 18 months. These must be kept in a secure place and destroyed by shredding after 18 months
- Follow the correct Authorization procedures
- Be alert to possible Credit Card fraud and report all instances
- For Card Not Present transactions, never store the CSC values (3-digit security codes on the reverse of the Visa, MasterCard or American Express credit cards) after a transaction has been authorised. Protect account and transactional information and your EFTPOS terminal by referring to the Authorization section of this guide

2.1 Settlement

Windcave operates on different settlement / merchant funding timing of each region.

Windcave process settlements only on business days. Settlement batches are dependent on the cut-off time for the batch; Windcave offer customized cut-off time for batch to suit merchant need for reconciliation with the end of the day.

2.2 Merchant Statement

At the end of each calendar month, Windcave will produce a summary of all Card Sales transactions which you have entered into during that month and of which Windcave has actual knowledge.

Windcave will not be bound, or in any way prejudiced, by any error, mistake, omission, or representation contained in any such statement account and transactional information and your EFTPOS terminal.

2.3 Merchant Service Fees (MSF)

Merchant Service Fee is the total fee paid by a merchant to an acquirer that covers all fees related to processing transactions for the merchant. The MSF can be different under various conditions which may be influenced by aspects such as number of transactions, average transactions size, value of international transactions, types of accepted payment methods, etc. See below for details on what fees make up the Merchant Service Fee.

Merchant Service Pricing Models:

Blended:

The Blended billing model is a single fee item that combines the Interchange Fee, Scheme Fee, and Acquirer Fee into one charge and is free from the potential variability of the other two pricing models available. It is a simplified model where the fee is simply a fixed percentage of total card sales. The monthly invoice does not show a breakdown of the fees as separate items. This pricing model is available in New Zealand, Australia, United Kingdom, and Canada.

- NZ: Windcave offers individualised rates under the Blended billing model covering Credit, Debit Contactless and International, applied at rates agreed with the merchant.
- AU/CA: Windcave offers individualised rates under the Blended billing model covering Visa/Mastercard Domestic and International, applied at rates agreed with the merchant.
- UK: Windcave offers individualised rates at both product (credit and debit) and transaction type (commercial/business and international) levels, applied at rates agreed with the merchant.

Interchange+:

The Interchange+ billing model has two components, Interchange Fee, and Acquirer Fee. Interchange Fee is a direct pass-through fee defined by the card schemes. Acquirer Fee combines both the Acquirer Fee and Scheme Fee into a single charge. Both Interchange Fee and Acquirer Fees charged for the transactions in the billing period are aggregated and listed as separate fee items on the monthly invoice issued in arrears. This pricing model is available in New Zealand, Australia, United Kingdom, and Canada.

Interchange++:

The Interchange++ billing model has three components, Interchange Fee, Scheme Fee, and Acquirer Fee. Interchange is a direct pass-through fee defined by the card schemes. Dependent on region, Scheme Fee can either be a direct pass-through fee similar to the Interchange Fee or an average cost, based on the charges received from Visa/Mastercard, as further detailed below.

- US: Scheme fee is directly pass-through
- AU/UK: Scheme fee is an average cost based on the charges received from Visa/Mastercard, this fee is reviewed annually starting from the 1st of July and applied on the 1st of August.

The Acquirer Fee is set by Windcave for services provided to the merchant for processing transactions. Interchange Fee, Scheme Fee and Acquirer Fee charged for the transactions in the billing period are aggregated and listed as separate items on the monthly invoice issued in arrears. This pricing model is available in Australia, United Kingdom, and United States.

Definitions:

Interchange Fee: Interchange Fee is a fee paid by a merchant's acquirer to a cardholder's bank (issuer), which is set by card schemes (Visa/Mastercard) for each card type. Interchange Fees can vary depending on the card type.

Scheme Fee: Scheme Fee is a fee paid by a merchant's acquirer to the card schemes, which is set by the card schemes.

Acquirer Fee: Acquirer Fee is a fee paid by a merchant to an acquirer (e.g. Windcave) to process the transaction for the merchant and can include Scheme Fees depending on the billing model (i.e., Interchange+).

International Fees (also referred to as International Service Assessment (ISA) fees): International Fees apply to any transaction where an International Card is used. An International Card is a card that is issued outside of the merchant's operating country. For EU merchants, an International Card is a card that is issued outside the EEA (European Economic Area). International Fees are applied on top of the base fees for the relevant transaction.

Pricing Model Breakdown:

Blended (1 fee item)	Interchange+ (2 fee items)	Interchange++ (3 fee items)
Single rate charged based on card type	Interchange (Pass Through)	Interchange (Pass Through)
	Acquirer Fee (Combination of Acquirer Fee and Scheme Fee)	Scheme Fee (Average Cost)
		Acquirer Fee

3 Connectivity

Merchants must allow connections to Windcave endpoints (services), for full details about connectivity and firewall/network considerations, please see Windcave | Connectivity

4 Transaction Processing

Transactions can be processes as either Card Present or Card Not Present.
This will be discussed with you during the application process and your facility approval confirmation will identify the types of transactions and card types you have approval to process.

4.1 Card Present (CP)

A Card Present transaction is one where the Cardholder and their nominated payment method are present during the transaction at your place of business. These transactions are processed via an EFTPOS terminal and can be processed with or without a PIN.

Insert
Cardholder presents their EMV (chip card) into the payment terminal, then follows any screen prompts to complete the transaction.

Contactless
Allows cardholders to pay by tapping their card on the contactless terminal.

Swipe

Allows cardholders to swipe the card's magnetic stripe through to the terminal to process the transaction.

QR Code
Allows payment scanning a unique QR code using an approved mobile wallet solution on your mobile device.

4.1.1 Contactless

Contactless is the latest form of Credit and Debit card acceptance and requires the cardholder to hold their card over the terminal until the transaction is accepted. You will need to have an EFTPOS terminal that accepts this kind of payment.

For security reasons, contactless payments do have a value limit that is set up per region. Please contact your bank to discuss these limits.
If the value of the transaction is greater than the limit, the cardholder will be prompted for card holder verification to complete the transaction. Card holder verification may be a PIN, signature, or device verification.

4.1.2 Standalone Payment Solution

A standalone payment solution means the terminal is not required to connect to any other software. Standalone terminals can be integrated with a POS system. You will need to manually enter the amount of the sale prior to passing the terminal to your customer.

4.1.3 Card Validation

To ensure a credit card is valid for payment when a transaction is initiated, the following checks should be made:

- Embossing the card should be even with all numbers the same size and shape.
- Check and confirm the expiry date on the card.
- Check the Cardholder name is embossed on the card, and it matches any other information provided.
- Check the 4-digit number printer below the account number is the same as the first 4 digits of the account number.
- Where an electronic microchip is embedded on the front of the card, check there is no evidence of tampering.
- Check for the 3-digit card security code next to the signature panel on the reverse of the card. These numbers are required for mail, telephone, and internet transactions.
- Check the card has a magnetic strip on the reverse side.

If you are suspicious of the card being a counterfeit, a transaction being fraudulent, doubtful of a signature or you are suspicious of a Cardholder and do not want to alert the Cardholder, note down as much information as you can and then call the card issuing bank after the Cardholder has left, and provide them with the information.

You may also contact the card issuing bank while the Cardholder is present, only if you feel safe to do so. It is important that you never compromise your own safety for card transactions.

4.1.4 Refunds

For refund transactions, Windcave strongly advises that merchants process the refund against the original transaction, this is known as a matched refund.

Merchants should never process a refund through cash or any other payment method as this increases the risk of chargebacks, and a potential loss for the merchant if a chargeback is raised (since the refund was not made to the original transaction using the standard matched refund process).

Merchants must ensure that reasonable steps are taken to validate the request for a refund. You may only process a refund by means of a transaction to a card on which a corresponding purchase was made. You must also ensure that refund cards are kept in a secure location and are only made accessible to staff who are authorised to perform refunds in a card-present environment.

4.1.5 Receipts

Receipts are available on all transactions processed through a terminal. You must ensure the 'customer copy' is available for the cardholder as a detailed record of their purchase.

You must retain the 'Merchant Copy' of all transaction's receipts in a secure location for 18 months.

4.1.6 Fall-Back

Fall-back occurs when a terminal may not read the card chip for various reasons including a damaged chip or damaged terminal.

Fall-back occurrences can be numerous and can be for genuine reasons:

- Faulty chip
- Faulty EFTPOS terminal
- Technical inoperability issues
- Poor merchant practice

Or deliberate:

- Disablement of EMV chip on card
- Disablement of EMV reader on EFTPOS terminal

On the rare occasion that an EMV card cannot complete the transaction via the card reader, if fall back is enabled you will be prompted to swipe the card. If a chip cannot be used correctly then a PIN should be requested, because the PIN is a higher form of validation than a signature.

Risks of operating in Fall-back mode
Transacting in Fall-back mode carries higher risk for the Merchant including:

- Higher risk of Chargebacks for merchant. As a lower form of security has been used to process the payment, the merchant has more liability for any transactions which are challenged by Cardholders as being incorrectly charged.
- Fines from schemes or disconnection. If a merchant continues to process high levels of Chargebacks, Visa will charge US$1 per transactions for excessive Fall-back transactions.

For merchants enabled for fall back, Windcave will contact you if you are processing higher than acceptable levels of Fall-back transactions. Should you continue to process high levels of Fall-back transactions; you may face disconnection.

4.1.7 Terminal Message Guide

All electronic transactions in obtain Authorization as part of the transaction process.
The authorized response is one of either:

Approved	Declined
The transaction has been authorized and processed. The goods or services can be supplied to your customer.	The transaction has not been authorized. The customer should provide an alternative form of payment or refer to the common error messages below.

4.1.7.1 Error Messages

For successful transactions the message is usually 'APPROVED', while unsuccessful transactions can exhibit a range of difference decline reasons. See below for possible terminal messages, descriptions, and the actions to rectify.

Terminal Message	Description	Action
Card Read Error	There is an issue reading the customers' card. Card may be damaged.	Retry or ask the customer to use an alternative card.
ICC Read Fail / Swipe Card	The terminal has failed to read the ICC chip card. ICC chip could be damaged on the card. If this error is happening on all cards, the terminal reader may be damaged.	Ask the customer to try another card and/or contact their bank.
ICC Declined	There is a problem with the operation of the chip card and terminal negotiation. The frequency of this error will increase when in offline mode (EOV) when the EMV chip decision forces online processing.	Try another card and/or contact their bank.
Invalid Card	There is a problem reading the card, or the card does not meet the conditions defined by the terminal. Card may be damaged.	Request the customer tries another card and/or contacts their bank.

Transaction Cancelled	The transaction has been cancelled by the user or operator.	Restart the transaction if required by the customer.
Timeout	Timeout – Declined: Transaction has timed out due to user inaction.	Restart the transaction if required by the customer.
Signature Declined	The signature provided as a form of verification is invalid and "No" was selected at the Signature authorisation stage (by operator). The transaction will be declined.	If you believe that this is a fraudulent transaction, follow your internal process for fraud detection.
Refer Issuer	The transaction was not approved and there is an issue with the card.	Ask the customer to try another card and/or contact their bank.

For consistent errors, further investigation, or assistance, please contact Windcave Support - Windcave | Contact

4.2 Card Not Present Transactions (CNP)

Card Not Present transactions are where both the Cardholder, and their credit card are not present at time of the transaction. These transactions may include mail order/telephone order (MOTO) and E-Commerce internet transactions.
Windcave take a strong view on CNP high-risk transactions such as MOTO, Manpan, rebilling and recurring (without 3DS or other means of cardholder verification).

4.2.1 E-Commerce Transactions

E-Commerce processing is set up for merchants who have a website and wish to sell goods or services via their website and to accept payments at the time of purchase. If you require an E-Commerce facility, please see the Section below for further information on what we can offer you.

There are several ways that Internet/E-Commerce transactions can be processed; please see below for more information.

4.2.1.1 Windcave Hosted

The Windcave Hosted Payment Page (HPP) is a payment page hosted on the Windcave secure payment network, merchants redirect their customers to the Windcave HPP to safely and securely enter their payment details before being redirected back to the merchant's website.

Commonly referred to as a hosted payment solution this integration method requires the least amount implementation effort and the lowest PCI compliance standard (PCI SAQ Level A) while still maintaining high levels of customization and functionality.

HPP is regularly used in online booking, shopping carts, bill payments, and many more applications where secure payment processing is required.

There are several options utilizing HPP as detailed below.

Payline

Payline is a browser-based application that can be used to process credit card transactions manually, process refunds, set up recurring payments and generate intelligent reports to aid with reconciliation and provide business intelligence.

It is most used by organisations that require a cost effective, quick, simple process for accepting credit card payments, and can also be scaled for all centres or organisations that require the ability to accept credit card payments in a card-not-present environment.
Payline is popular with businesses that have traditionally telephoned or faxed credit card details to the bank for processing, and are now at the stage where real-time, processing, and next-day settlement of funds is required.
For more information on Payline, please see - Windcave | Payline

Paylink

The Payline solution allows merchants to send a secure Hosted Payments Page (HPP) link directly to customers via Email or SMS. Virtual terminals can also be used to process payments for MOTO transactions.
With support for 3DS, the HPP provides merchants additional protection against chargebacks when processing MOTO (Mail Order Telephone Order) or manual payments, reducing the risks and cost of accepting credit card payments.
For more information on Paylink, please see - Windcave | Paylink

Payform

Payform provides an off-the-shelf ecommerce payment solution for merchants who may not have the expertise/resource available to complete a full Hosted Payment Page (HPP) API integration into their website.
With support for 3DS, the HPP provides merchants additional protection against chargebacks when processing payments, reducing risks and cost of accepting credit card payments.
When implementing Payform merchants can choose to redirect from their website or send the customer the static Payform link, this link can optionally be prepopulated with order details or allow the customer to enter details on the Payform page. After inputting details, the customer will be redirected to the HPP to enter sensitive payment information and securely process their payment.

Account2Account (A2A)

Account2Account (A2A) provides a solution for merchants to accept payments directly into their bank account by creating a one-off online payment using the customer's online banking portal. This facility is already widely used where a merchant provides their bank account details and customers pay by creating a one-off payment via online banking.

The key difference is that with A2A, the one-off payment is created on a secure page hosted by Windcave. Windcave can authoritatively inform the merchant when a payment is created, and the customer is redirected back to the merchant's website once payment is created. This means that the merchant website receives the transaction outcome in real-time. Goods can then be shipped on the receipt of funds to the merchant's bank account (or at the merchant's discretion).

4.2.1.2 Merchant Hosted

Form Post

The Merchant Hosted Payment Page (MHPP) form post integration utilizes a client-side HTML form, the secure card data is securely posted from the cardholder's browser directly to the Windcave Host. With the MHPP form being hosted on the merchant's website it provides a merchant-controlled UI experience for users.

This method may be preferred for merchants as there is no redirection for their customer, meaning they do not need to leave the merchant website to enter their payment details. This however will increase the PCI SAQ scope (SAQ A-EP) and this integration method is not supported by all acquirers, it is strongly recommended that you discuss with your chosen acquirer before proceeding with this integration method.

For merchants to be able to securely post their users sensitive payment information from the client-side form directly to Windcave; a session is created in the Windcave host for each payment.
New sessions are created on request and triggered by the merchant web server sending a create session request, the newly created session will be given a session id which is used to reference the user's payment.

AJAX
The Merchant Hosted Payment Page (MHPP) AJAX post integration utilizes a client-side form, the secure card data is securely posted from the cardholder's browser directly to the Windcave Host. With the MHPP form being hosted on the merchant's website it allows merchants to offer a more native payment page experience.

AJAX or Asynchronous JavaScript and XML involves the loading of data in the background and displaying it on the webpage without reloading the whole page.

This method may be preferred for merchants as there is no redirection for their customer, meaning they do not need to leave the merchant website to enter their payment details. This however will increase the PCI SAQ scope (SAQ A-EP) and this integration method is not supported by all acquirers, it is strongly recommended that you discuss with your chosen acquirer before proceeding with this integration method.

Server-side Post / Create Transaction
Please note this section is documented in terms of purchase transactions, however Auth/Complete and Validate transaction types are also supported in these examples.
The Merchant Hosted Payment Page (MHPP) server-side post integration utilizes a server-side form, the secure card data is posted from the merchant webserver directly to the Windcave host. As the MHPP is hosted on the merchant's website it allows merchants to offer a fully native payment page experience.

This method may be preferred for some merchants as the fully native payment page provides further control and capture of full card details. This however will increase the PCI SAQ scope (SAQ D) and this integration method is not supported by all acquirers, it is strongly recommended that you discuss with your chosen acquirer before proceeding with this integration method.

Please note merchants may be requested to provide their PCI-DSS Attestation of Compliance (AOC) to Windcave before proceeding with integrating to this method, a Non-Disclosure Agreement (NDA) may be put in place prior to sharing the PCI-DSS AOC.

To learn more about Rest API's and its' offerings, please see Windcave | Rest API

4.2.1.3 Recurring and Tokenization

The Windcave Recurring Billing software enables any business to automate their credit card billing cycle using several PCI DSS compliant options, which are both secure and easy to use. Depending on the businesses' software environment, we can provide a range of software-based solutions to take the work and risk out of receiving regular credit card payments.

4.2.1.4 Batch

Windcave provides several options for merchants who have a need to process large numbers of transactions quickly, easily and in a PCI DSS compliant environment. The Batch Processor uses military grade encryption (3DES) and securely authorizes transactions in real time. The software is capable of processing thousands of transactions as a single batch, this will save any business valuable time, effort, and staff resources by moving away from having to manually process transactions individually.

4.2.1.5 3DS

3DS or 3D Secure, are authentication tools designed to combat fraudulent online transactions by shifting liability of chargebacks onto the card issuing bank. 3DS reduces the friction of authentication by increasing data sharing between merchants and card issuers in a non-intrusive way and supporting modern authentication methods such as 2-factor authentication (2FA).

Frictionless Flow	Friction Flow
The system recognizes and verifies the user's device and data are exchanged in the background. There are no additional requests from the site to the payment platform. Using the frictionless flow, the issuer can confirm the transaction as it considers as a low risk and no challenge will be given to the user.	A friction or challenge flow is when the system doubts the identity of the user and requires an additional one-time password or bio-metric verification. The user is re-directed to the card issuer's ACS (Access Control Server) page to enter the necessary information.

3DS covers the MasterCard SecureCode and Visa's verified by Visa (VbV) initiatives. These were designed to verify the identity of the Cardholder for online purchases and assist merchants to minimize their exposure to fraud by allowing Cardholders to choose an online PIN or Password that confirms they are the real owner of the card.

3DS is not a failsafe tool. It is your responsibility to satisfy yourself that the Cardholder is who they say they are. Cardholders can still claim 'goods not received/defective', 'not as described merchandise' or that credits were not processed. Please view the Chargeback section of this guide for information on how to protect your business and what to do if requested to provide information for a Chargeback.

As part of Windcave' continuing efforts to promote best practice solutions, our Hosted Solution PxPay 2.0, Hosted Payment Page (HPP), AJAX and PxPost options allow merchants to participate in the Verified by Visa and MasterCard SecureCode schemes at no additional cost.

For more information on 3DS or authentication options, please contact your Windcave Sales team at sales@windcave.com or the Windcave Support team - Windcave | Contact

4.2.2 MOTO (Mail Order/Telephone Order)

MOTO means Mail Order / Telephone Order. With MOTO transactions, the merchant never receives a signature or PIN from the customer, but only the credit card number and expiration date and this is manually entered to process the payment.

MOTO and Manpan are non-qualified high-risk transactions, these can attract more fees and are at a greater risk of chargebacks.

Depending on the merchant requirements, MOTO transactions can be processed through Windcave's web-based payment manager Payline following a simple PayMOTO process.
For more information on Payline, click here. Alternatively, contact your Windcave Sales manager for more information – sales@windcave.com

IMPORTANT: **Manpan (manual) transactions are the most high-risk transactions; If the transaction is processed via MOTO/Manpan, Merchant must ensure proper due diligence as Windcave will not be representing the case (As its 100% Merchant Liability) ***

***If the merchant chooses to represent the case which has come through under fraud, they are advised of the additional costs (charged by the schemes) prior to following through with the representment.**

Alternatively using a Windcave Hosted Payment Page (HPP) guarantees a secure payment process while still allowing customization – See here for more information on HPP

4.2.3 Processing a Refund

Refunds can be processed through the Windcave Payline portal. Merchants can access this portal with their assigned user credentials and follow the refund process prompts to complete these transactions.

5 Surcharging

If a merchant decides to enable a surcharge to their transactions, the surcharge amount should be reasonable and not greater than the cost of credit card acceptance.

Please note for merchants operating in the US, surcharging is not allowed or restricted in most states. For merchants operating in Australia, the merchant cannot surcharge more than their cost of credit card acceptance, except in the case of American Express. The merchant may not apply a surcharge American Express Cardholders in Australia that is more than any surcharge the merchant applies in respect of other credit cards.

For merchants operating in New Zealand, the merchant may not surcharge more than their cost of credit card acceptance, except in the case of American Express. The merchant may not surcharge American Express Cardholders in New Zealand.

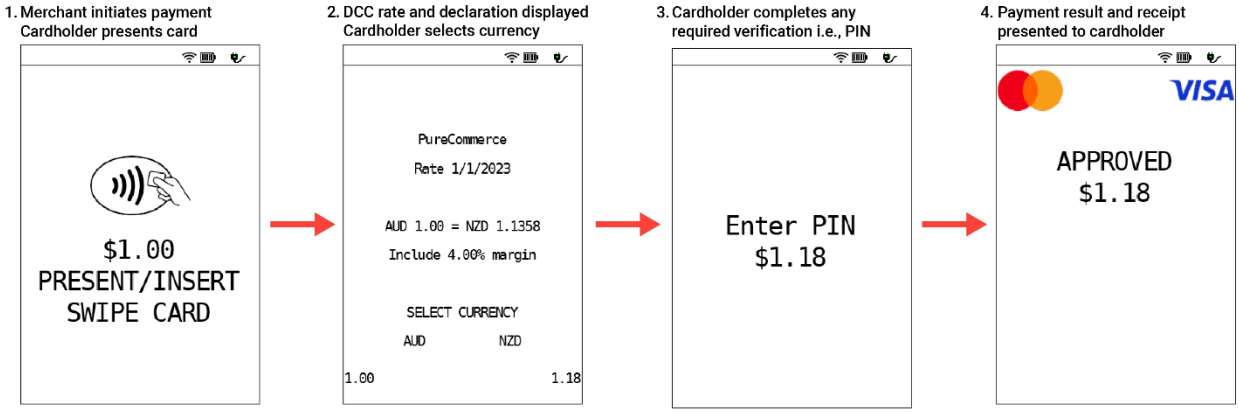
Please refer to your local laws and regulations on surcharging, or contact your Windcave Sales Account Manager for further information – Sales@windcave.com

6 Dynamic Currency Conversion (DCC)

This section includes examples of a Dynamic Currency Conversion (DCC) transaction flow as well as outlining merchant requirements and best practices when offering DCC to your customers.

6.1 DCC Transaction Flow

Outlined below is an example of a DCC transaction flow.
Please note that the screen appearance may differ slightly between different payment terminals.



6.2 Merchant Requirements

The payment schemes perform monitoring and unscheduled audits on-site for DCC merchants; this is to confirm they are compliant with meeting DCC requirements.

Merchants found to be non-compliant may be issued a significant fine and have their ability to process DCC transactions revoked.

```
Merchant Name
Merchant Address

*---------EFTPOS----------*
MERCHANT     *********01234
TERMINAL             0001
01 Jan 23 12:37      CREDIT
VISA            ICC CONTACT
AID          A0000000000000
APP LABEL              Visa
CARD        ************1234
PAN SEQ Number         01
RRN             000000000000
AUTHORISATION        123456
REFERENCE            123456
PURCHASE           AUD1.00
TOTAL              AUD1.00

TRANSACTION CURRENCY
                   NZD1.14
     1 AUD = NZD 1.1003
MARK-UP PERCENTAGE   4.0000

 [X] I have been offered a
  choice of currencies and
 have chosen to accept DCC
  and pay in NZD. Currency
 Conversion is provided by
       Merchant Name

         APPROVED

       PIN VERIFIED

*-------------------------*
       CUSTOMER COPY

       PLEASE RETAIN
     FOR YOUR RECORDS
```

Outlined below are key responsibilities merchants must follow to ensure you are compliant with DCC requirements:

- Merchants must NOT steer or influence the cardholder's decision of currency used; this must be their own choice.
- A DCC receipt must be provided to the cardholder where possible.
- Outlined to the left is an example of a correctly formatted DCC receipt. If your receipts have any of the below issues, please contact Windcave and/or your Point of Sale provider to remedy as soon as possible:
  - Exchange rate and DCC declaration missing from DCC transaction receipt
  - Only POS receipt printing, no EFTPOS receipt is printed
  - Mark-up percentage is missing unit of measurement, i.e. does not show % symbol or word, only a value

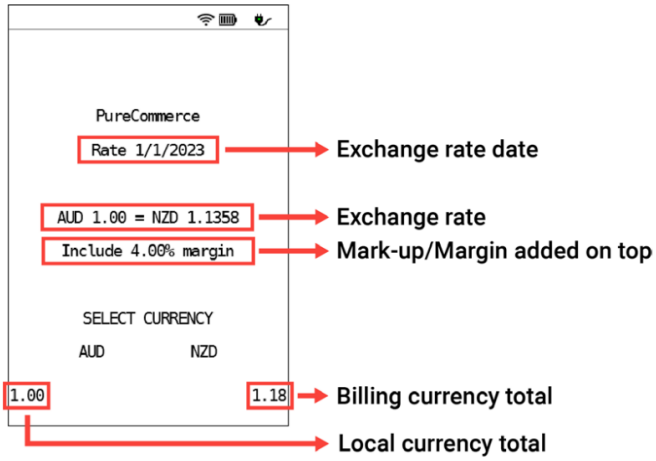
6.3 Best Practices

The below outlines merchant best practices for DCC transactions.

If questioned, merchant staff should be able to explain DCC and highlight the below key items for the cardholder to review:

- Transaction amount in local currency
- Transaction amount in billing currency (cardholders home currency)
- DCC exchange rate offered (conversion rate from local currency to billing currency)
- Mark-up percentage/fee that will be included when paying in billing currency

All of the above information should be presented on the screen of the Windcave payment terminal as per the image below:



Merchants should ensure their staff have been provided training and have a strong understanding of DCC requirements and best practices.

7 Offline Processing

Electronic Offline Voucher (EOV), also known as Offline Mode, is a feature that allows merchants to continue accepting payments when the terminal is unable to communicate with the baking systems.

When is Offline Mode available?

The Windcave terminal can enter offline mode under a few circumstances:

- Network communication issues
- Windcave Host unavailable

Offline mode is designed to only be used as a final resort to processing payments in events of loss of network communications. It is recommended that merchants also implement backup/redundant network communication systems that be utilized to maintain communications to the Windcave host where possible.

IMPORTANT: Not all cards are supported for EOV transactions. This is determined by the card issuer.

Offline Processing Limits

Limits are put in place to help protect merchants when processing offline transactions due to the

inherent higher risk. Limits are set by the merchant acquirer/processing gateway and are configured based on an agreed level of acceptable risk between the merchant and their acquirer.

Risks	Benefits
• Limits and restrictions are applied to transactions processed offline which may affect acceptance rates • Not all cards allow for offline processing. EMV (chip) cards have their own limits and can restrict or even prevent the processing of offline payments for the card • Not all transaction types are allowed in Offline mode	• Reduces the impact of major network outages by allowing merchants to continue processing as many payments as possible during the outage or connectivity errors • Vouchers are processed in a safe and secure manner. EOV payments are stored securely on the Windcave terminal and uploaded once internet connectivity has been restored

How does Offline Mode work?

Windcave terminals will enter offline mode when one of the below conditions is met and offline processing is enabled for the terminal:

- Two transactions fail to network timeouts
- A loss of network communications is detected
- The Windcave host cannot be reached

Once in offline mode, merchants can initiate payments in the same manner however may be prompted to acknowledge before processing the payment offline. Once processed, the merchant will be prompted to obtain and verify the cardholders' signature begore the payment is finalized and stored offline for later upload.

While in offline mode, the terminal will continue to check for communications every 10 minutes. If the connection is restored, the terminal will go back to online mode and upload any transactions processed in offline mode to the Windcave host.

EOV display messages

EOV transactions may show the below messages on the terminal.

Display Message	Description / Action
CALL HELP DESK – OFFLINE EXCEEDED	This error will display for 3 reasons: 1. Maximum offline transactions reached 2. Maximum offline minutes reached 3. Maximum offline amount reached
OFFLINE ALREADY STORED	This error will decline the transaction due to: 1. Daily transaction limit reached 2. Session Velocity reached 3. Daily Velocity reached
MAX AMOUNT EXCEEDED	This error will decline the transaction due to: 1. Offline Purchase Limit for Credit reached 2. Offline Purchase Limit for Debit reached

CARD NOT ALLOWED	This error means the terminal is not configured to accept this card is EOV mode
ICC DECLINED	This error means the EMV chip has declined the transactions – this is due to limitations or restrictions placed by the card issuer and is the decision, therefore cannot be processed

For assistance on error messages for EOV transaction processing, please contact Windcave Support for assistance - Windcave | Contact

8 Authorization

8.1 Card Present (CP)

All electronic transactions obtain authorisation automatically as part of the transaction process. The authorisation process provides a check at the time the transaction is processed, on whether the Card number quoted is a valid card. It checks the availability of funds and establishes whether the card has been reported lost or stolen.

It does not establish if the Cardholder is genuine. It is your responsibility to establish that the purchaser is who they say they are and are authorized to use the card presented for payment.

Please note: An authorisation does not guarantee payment. If at a later date the transaction is found to be an invalid transaction, it may be charged back to you. See the Chargeback section for further information.

8.2 Card Not Present (CNP)

Authorization is obtained automatically as part of the transaction process for all electronic transactions. You must ensure that the Cardholder provides you with all the details necessary to properly authorize the transaction.

It is also advisable to obtain:

- A contact phone number (not mobile).
- The name of the bank that issued the card.
- For mail orders, ensure that you obtain a signature on the order form.
- A contact phone number (not mobile).

Remember: it is your responsibility to ensure the Cardholder is who they say they are.
Acceptance of Card Not Present transactions must be explicitly stated in your facility approval confirmation with Windcave Merchant Services.

Please call Windcave to discuss the acceptance of card details from additional channels.

9 Transactional Fraud Prevention

Fraud can be committed by persons using stolen credit card details, your employees or both colluding. This can cause significant financial and reputational loss for your business.

To minimize the risk of fraud, use all security functionality offered:

- Card Present – Chip and PIN in preference to signature
- Card Not Present – Fully hosted with 3DS (v2)

What can I do?
It's your responsibility to verify to your own satisfaction the identity of a customer prior to the supply of goods and services. The following are suggested checks:

- Ask for comprehensive customer details and validate these. Obtain the customer's full name, address, and home phone number.
- Do an order confirmation – telephone the customer sometime later to confirm order details before delivering. Where the customer is not aware of the order or cannot confirm the details, issue a refund on the card and do not deliver the goods.
- Partial refund – make a small refund (example 37 cents) back to the card. Ask the customer to access their account and state the amount refunded.
- Ask the customer where their card was issued and by which bank. You can verify these details on websites such as binbase.com and exactbins.com
- Ask the customer to show their credit card and driver's license (where possible) as identification on the delivery.
- Never deliver the goods to post office boxes.
- Never leave the goods at unattended premises.
- Always ask for the card expiry date.

If you have any doubts and cannot verify any of the points above, we recommend that you issue a refund to the card and seek alternative forms of payment until a trading relationship is established. Never refund to a different card, and never refund or forward funds to a bank account or via Telegraphic Transfer. Receiving authorization, including funds deposited to your account does not guarantee payment. Transactions may be challenged up to 180 days after they have taken place and funds may be reversed from your account.

9.1 Card Not Present Fraud

Accepting payment for goods in a Card Not Present manner comes with a higher level of risk than Card Present transactions. Please see Transaction Processing section of this guide.

Stay alert for the following fraud indicators. Any one of these factors could indicate a higher degree of fraud risk.

1. First-time customers. Criminals are always looking for new Merchants to steal from.
2. Larger than normal orders. Stolen cards or account numbers have a limited life span, criminals need to maximise the size of their purchase.
3. Orders that include several of the same item. Having multiples of the same item increases a criminal's profits.
4. "Rush" or "overnight" shipping. Criminals want their fraudulently obtained items as soon as possible for the quickest possible resale and aren't concerned about extra delivery charges.

5. Shipping outside the Merchant's country. There are times when fraudulently obtained goods and services are shipped overseas. If most of your orders come from overseas, ensure that you take care to validate the legitimacy of the order.
6. Inconsistencies. Information in the order details, such as billing and shipping address mismatch, email addresses that do not look legitimate and an irregular time of day when the order was placed.
7. Multiple transactions on one card over a very short period. This could be an attempt to "run a card" until the account is closed.
8. Shipping to a single address, with transactions placed on multiple cards. This could involve an account number generated using special software, or even a batch of stolen cards.
9. Multiple transactions on one card or a similar card with a single billing address, but multiple shipping addresses. This could represent organised activity, rather than one individual at work.
10. Orders from internet addresses that make use of free email services. Customers who sign up for free email services are not required to provide proof of their identity or address in order to establish an account, so it is important to take extra steps to validate the person placing the order.

Certain industries have been identified as higher risk for fraudulent activity. If you are in one of the following industries, please take extra care with all internet transactions.

- Electronics stores
- Computer software stores – including digital downloads
- Telecommunication services
- Food stores
- Gift cards – including prepaid debit cards
- Novelty stores
- Sporting goods stores
- Jewelry stores

9.2 Card Present Fraud

Card Present fraud still occurs. Here are some common signs which should raise alarm for you:

- Larger than normal orders. Stolen cards or account numbers have a limited life span, criminals need to maximise the size of their purchase.
- Price is not considered. Criminals will often not haggle on price as they want to complete the purchase in as little time as possible.
- Colour, design is not considered. Criminals will often not worry about colour, or other flexibility in a product as they want to complete and obtain the goods in as shorter time as possible.
- Inconsistencies. Information in the order details such as billing and shipping address mismatch, email addresses that do not look legitimate.
- Multiple transactions on one card. If a card is stolen the purchaser will not know the limit and will purchase until the card has reached its limit.
- Split transactions on multiple cards. If the cards are stolen the purchaser will attempt to spread a large purchase over a number of cards as they do not know the credit available on the cards.
- Damaged cards. Always use the highest form of security. Cards can be damaged so the Chip or Magnetic Stripe will not work in an EFTPOS terminal reducing the option from PIN to Signature, or Chip to Magnetic Stripe. Never accept payment via a damaged chip card without a PIN, and train your staff to ask for PIN on all transactions, or to verify magnetic stripe with a second form of ID – the details of which can be written on the reverse of the merchant copy EFTPOS receipt. Second forms of ID may be a photo Driver's License, Passport, or any other ID that gives you comfort that the transaction is being completed by a person who is entitled to the card.

- Last minute shopper. Purchaser arrives at the end of the day and flusters staff with a rush order and any of the above signs.

9.3 Transaction Fraud

Higher risk transactions

The following types of transactions are examples of those that carry higher risk. Extra care should be taken when processing transactions of this nature:

- First time customers.
- International orders - particularly South-East Asia and Africa.
- Email orders especially from a free email address such as Yahoo!, Hotmail, or Gmail.
- Card Not Present transactions, including email, internet, mail, and telephone orders.
- Any transaction where the card is not swiped, inserted, or tapped on an EFTPOS terminal.
- Transactions which are manually keyed into an EFTPOS terminal.
- Manual transactions where no authorization has been obtained.
- Manually entered transactions where the card number is manually keyed into the terminal instead of swiping or inserting the card.
- Transactions where an authorization has not been obtained.

Lower risk transactions

The following types of transactions are lower risk:

- Card Present transactions where the transaction is completed through the EFTPOS terminal or an imprint of the card as well as signature and authorization is obtained.
- Internet transactions authenticated via Verified by Visa or MasterCard SecureCode, or alternative forms of 2-factor authentication

Note: All transactions carry a level of risk. Before you accept payments, you need to make yourself familiar with these risks.

9.4 Employee Fraud

Typical ways employees perpetrate credit card fraud:

Process a credit transaction to their own account

Employees may issue credits to their own credit card or to an accomplice's card using the merchants EFTPOS terminal using funds meant for the merchant's direct deposit account.
Windcave recommend the use of Payline for refunds, as refunds can only be made to the original card, and for a maximum of the original amount.

Record card numbers

Employees may pocket receipts left behind by Cardholders or may copy card numbers onto a separate piece of paper. Systems that truncate the card number on the customers receipt can help your business avoid this type of fraud.

Use a card skimmer

A dishonest employee can steal valuable information off a customer's card though use of a small, battery-operated 'card skimmer'. This hand-held device reads a cards magnetic stripe and records the Cardholder data for later download to a computer. From there, the numbers can be used to make unauthorized purchases or create counterfeit cards.
Despite the opportunity for employee fraud, you as a merchant are not totally without protection. Most terminals or transaction software tools allow you to require a password in order to process a credit transaction, and there are a number of other tactics you can use to prevent employee fraud.

These include:

- Reconciling your work daily rather than monthly
- Password protecting the refund function on your credit card terminal
- Secure your terminal outside normal business hours
- Have a separate authorizer of refunds in addition to the person who physically processes a credit
- Make sure all credits have accompanying internal documentation of customer information (name and contact information) and reason for return or dispute.
- Match credits to returned or disputed goods or services, verify with customers that they did actually return/dispute goods or services.
- Have more than one person review monthly statements.
- Send all credit transactions to a central office for review.
- Review credits daily, or have a trusted employee do the review.
- Fully investigate credits without matching sales.
- Review any batches with negative dollar amounts (more credits than sales).
- Conduct regular internal audits at random times and intervals.
- Audit bookkeeping and accounting processes quarterly.
- Track credits by card number, terminal number, employee, frequency, and dollar amount (exception-based reporting).
- Review any volume spikes in credit/return/dispute activity.
- Protect your passwords and verify internal access controls for online account reporting and checking account change requests. 3DS is not a failsafe tool. It is your responsibility to satisfy yourself that the Cardholder is who they say they are.

10 Chargebacks

A Chargeback is a reversal of a credit card transaction previously credited to your account. Generally, if a Cardholder disputes a transaction and you do not have sufficient evidence to show that the Cardholder authorised the transaction, the liability for the Chargeback will then rest with you. This means that the original transaction is reversed, and you will not receive payment for the goods or services you may have already delivered. You may also be required to pay fees for investigating and processing the Chargeback. If you are requested to present information for a Chargeback (where a purchase is being disputed by the Cardholder) information that will assist includes:

- Evidence that the transaction was completed by a member of the Cardholder's household.
- Details of order including Cardholder's name, delivery address and what was purchased.
- Signed order form.
- Details of order placed, delivery information (date and address), and signed delivery docket to confirm goods have been received.
- Evidence, such as photographs or emails, to prove a link between the person receiving the merchandise and the Cardholder, or to prove that the Cardholder disputing the transaction is in possession of the merchandise.
- Details of any credits you have processed to the original card used in the transaction.

Note: Providing this information does not guarantee funds will not be deducted from your Merchant Account in accordance with the Card schemes terms and conditions but does assist Windcave in answering the dispute on your behalf.

10.1 Common Chargebacks and Mitigation

If you are contacted for information regarding a transaction that been charged back, you will need to provide the following information as a minimum:

Chargeback reason: Goods not received/defective, not as described merchandise

- Obtain details of order placed, delivery information (date and address), and signed delivery docket to confirm goods have been received.
- Evidence, such as photographs or emails, to prove a link between the person receiving the merchandise and the Cardholder, or to prove that the Cardholder disputing the transaction is in possession of the merchandise.

Chargeback reason: Credit not processed

- Obtain details of any credits you have processed to the original card used in the transaction.

Please note: It is important to refund to the original card only, as refunds processed in any other manner to other cards or accounts will not be valid.

To minimise your Chargeback risks, talk to you web developer to see if one or more of the following can be automatically captured and stored:

- Customer name, shipping address and what was purchased.
- Evidence that the transaction processed 3DS authorization.
- Purchaser's IP address.
- Purchaser's email address.
- Description of the goods downloaded, if applicable.
- Date and time goods were downloaded, if applicable.
- Proof that the merchant's website was accessed for services after the transaction date if this is a subscription purchase.

Mail/Telephone order transaction:

- Signed order form.
- Details of order including Cardholder's name, delivery address and what was purchased.

There are business processes you can implement to help your business reduce the likelihood of receiving a Chargeback. You can reduce the risk of Chargebacks caused by customer disputes by keeping good records. This will help you to find specific transactions quickly and easily.

You should include all of the following information in your invoices, contract, and promotional materials:

- Your business name as it will appear on the Cardholder's statement.
- Your business address.
- Customer service contact numbers.
- A complete description of goods and services provided.
- A specific delivery time.
- Details of your return and cancellation policy.
- Details of debit dates for regular instalments such as memberships or subscriptions.

You can also reduce the risk of Chargebacks resulting from fraudulent use of cards by requesting the card verification code, or CVV2/CVC2, and using a security program such as MasterCard SecureCode or Verified by Visa.

If you are contacted in relation to a Chargeback, it is your responsibility to provide information to Windcave to assist in providing evidence to the card issuing bank on your behalf. Failure to provide

information in the required time frame (normally 10 business days) can result in the Chargeback being processed in accordance with the Card schemes' requirements.

If, after Windcave have submitted your documentation to the Cardholder's bank, we are still unable to satisfy the Cardholder bank that the transaction was valid, Windcave will confirm this in writing advising a date for the debit to be processed for the full amount.

Manual Transactions (MAN PAN):

This service enables manual transactions (MAN PAN) to be performed directly via the Pinpad rather than through the Point-of-sale application. There are two variants of this service:

1. Only the PAN and CSC entry is performed via the Pinpad. The CSC indicator selection (e.g., mail order, telephone order), is managed by the POS.
2. The CSC selection prompts are disabled, and hard-coded values configured in PXPP. This option simplifies POS integration and allows backwards compatibility with existing integrated POS.

MAN PAN allows advantages including:

1. Simplified Process – The entire process can be performed via the pinpad
2. Increased Security – The POS does not need to manage the PAN entry and the associated risks (The pinpad capture of the card number is now secured in the same way as capture via card swipe, i.e. is not made available to the PC in clear text at any stage.
3. Simplified POS integration – MAN PAN can be supported out of the box for POS which are integrated with custom UI.

The PAN entry prompt is triggered by a manual button UI press, or, if the clear/back button on the Pinpad is pressed while on the swipe card stage.

IMPORTANT: Manpan (manual) transactions are the most high-risk transactions; If the transaction is processed via MOTO/Manpan, Merchant must ensure proper due diligence as Windcave will not be representing the case (As its 100% Merchant Liability) *

***If the merchant chooses to represent the case which has come through under fraud, they are advised of the additional costs (charged by the schemes) prior to following through with the representment**

When can a Chargeback occur?

A chargeback can be initiated when:

- The goods or services supplied are illegal or prohibited
- The card was not valid at the time of the transaction
- The cardholder disputes liability for the transaction for any reason
- The cardholder did not authorize the transaction
- Authorization for the transaction was declined for any reason
- The sales receipt has been altered without the cardholder's authority
- It was processed to your own credit card
- You breach a term of your Merchant Agreement
- The transaction amount is greater than your floor limit and you did not get an authorization
- If represents the refinance of an existing debt or the collection of a dishonest cheque

11 Business Protection

11.1 PCI DSS

The Payment Card Industry Security Standards Council is an institution which includes MasterCard, Visa International and American Express whose aim is to enhance credit card payment security.

It aims to achieve this goal through the mandatory adoption of the PCI Data Security Standard (PCI DSS) by all businesses that store, process and/or transmit credit card scheme data (card numbers and other sensitive information).

11.1.1 PCI DSS Requirements

Goal	PCI DSS Requirements
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect Cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder data	3. Protect stored Cardholder data 4. Encrypt transmission of Cardholder data across open, public networks
Maintain a vulnerability management programme	5. Use and regularly update anti-virus software or programmes 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to Cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to Cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and Cardholder data 11. Regularly test security systems and processes
Maintain an Information Security policy	12. Maintain an Information Security Policy

How to minimise your PCI DSS risk?

The best way to lower your reporting obligations is to remove the presence of credit card numbers from your business. PCI approved, a fully hosted payment solution such as PxPay 2.0 will capture the credit card numbers and process this information for you. This prevents any card numbers, or other details, being available to staff within your business, and lowers risk of card numbers being stolen via web and IT attacks.

As a Merchant accepting Visa, MasterCard or American Express, you must not store or retain any sensitive data post authorisation which includes but is not limited to:

- Primary Account Number
- CVV2/CSC2/CVC2
- Customer Pin Number
- Magnetic stripe data.

This includes cards used in POS readers for obtaining customer name, or other details in Hospitality POS, bar tabs, retail POS, loyalty, or any other magnetic stripe reader.

Please see the links below for more information from Visa, MasterCard and American Express:
Visa PCI DSS Compliance:
https://www.visa.co.nz/support/small-business/security-compliance.html

MasterCard Site data programme (SDP):
https://www.mastercard.com/global/en/business/overview/safety-and-security/security-recommendations/site-data-protection-PCI.html

American Express data security requirements:
http://www.americanexpress.com/dsr

11.1.2 Protection

The benefits of PCI DSS include:

- Reducing the risk of credit card fraud.
- Avoiding fines, penalties and costs related to credit card security breaches and non-compliance.
- Increasing consumer confidence in credit card payments.
- Reducing your business' exposure to potential lost revenue as a result of fraud.

11.1.3 PCI DSS Compliance Reporting

PCI DSS Merchant Level	PCI DSS Requirements
Level 1 (More than 6 million card transactions annually, any method of acceptance)	• Annual On-site review by a Qualified Security Assessor (QSA) or Internal Security Assessor (ISA). • Quarterly network vulnerability scans (if applicable) by an Approved Scanning Vendor (ASV).
Level 2 (More than 1 million but less than 6 million card transactions annually, any method of acceptance)	• Merchants completing SAQ A, A-EP or D are required to engage a QSA or use an ISA for annual compliance validation. • Merchants completing any other SAQ's may undertake a Self-Assessment without input from a qualified QSA or ISA. • Quarterly network vulnerability scans (if applicable) by an Approved Scanning Vendor (ASV).
Level 3 (More than 20,000 but less than 1 million e-commerce transactions annually.)	• Annual completion of a Self-Assessment Questionnaire (SAQ). • Quarterly network vulnerability scans (if applicable) by an Approved Scanning Vendor (ASV).
Level 4 (Less than 20,000 e-commerce transactions annually)	• Annual completion of a Self-Assessment Questionnaire (SAQ). • Quarterly network vulnerability scans (if applicable) by an Approved Scanning Vendor (ASV). • Validation for Level 4 merchants is optional in certain regions.

To assist you with validating your PCI DSS compliance requirements, your organisation has been pre-registered for a SecureTrust PCI Manager account. If it is necessary for your organisation to validate it's PCI DSS compliance requirements, the authorised contact for your organisation will receive a registration email from SecureTrust inviting them to access the portal.

Level 1 and Level 2 merchants who are required to use a QSA or ISA to validate their PCI DSS compliance are expected to upload the necessary documents on to the portal (e.g., Report on Compliance, SAQ, ASV scans) to demonstrate their compliance.

Level 2 merchants who may self-asses and Level 3 & 4 merchants validate their PCI DSS requirements by completing an SAQ and vulnerability scans if applicable. SecureTrust is an Approved Scanning Vendor (ASV), and their scanning tool is accessible via the portal.

The exact requirements that you will have to satisfy are determined based upon the services that you are receiving from Windcave.

It is a contractual obligation for your organisation to validate your PCI DSS compliance requirements. Penalties may apply if you fail to complete the program within 3 months of receiving the pre-registration email from SecureTrust.

The card schemes (e.g., Visa and Mastercard) can also apply penalties and fines for non-compliance with PCI DSS. As per Windcave's agreement with your entity, if a card scheme imposes a monetary fine in relation to non-compliance by the merchant, Windcave will pass on the fines to the merchant.

A list of PCI DSS approved QSA's can be found via the following link:
https://listings.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

A list of PCI DSS Approved Scanning Vendors (ASV) can be found via the following link:
https://listings.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors

11.1.4 Obligation

PCI DSS applies to any party that interacts with credit card numbers in any manner at any point in or after the transaction has been completed. This includes any interface, PC, web page that may see, pass, transmit, collect, process, or store card numbers. All these parties in the payment process must be PCI DSS compliant regardless of the size of the business or volume of transactions made. It is the responsibility of the Merchant to ensure all parties in their payment process are PCI Compliant.

For more information on PCI compliance and reporting requirements, please follow the link below:
https://www.pcisecuritystandards.org

11.2 Brand and Business Risk

What is brand and business risk?

Brand risk is any product, action, content, or service which has the potential to damage the reputation of Windcave, MasterCard, Visa or American Express. If Visa, MasterCard, American Express or Windcave deem a Merchant as potentially damaging their brand, the Merchant can have their merchant facility removed without notice, for breach of terms and conditions.

11.2.1 Unacceptable businesses

The following examples include some merchant categories that are banned by Visa, MasterCard and American Express:

- Counterfeit and copyright infringing merchandise
- Child pornography
- Illicit websites depicting violence and extreme sexual violence
- Potentially deceptive marketing practices
- Online gambling
- Purchase or trade of media or activities related to child pornography, bestiality, rape (or any other non-consensual sexual behaviour) or non-consensual mutilation of a person or body part

The following business types will need to be monitored and may be required to pay a fee for annual registration with Visa and MasterCard (including but not limited to):

- Drugs (prescription/pharmacy only/restricted medicine)
- Tobacco product sales
- Pay per call/minute services (horoscopes/ chat lines/marketing services)
- Internet hosting/access/data storage
- Social media sites
- Any business that may be deemed brand damaging to Windcave, Visa, MasterCard or American Express
- Cyberlockers (internet-based data storage facilities)
- Software suppliers
- Sale of Government forms

Please note: If you are selling internationally then your products must be legal in:

- The country the credit card was issued in
- The country the goods were ordered from
- The country the goods are being sent to

Legality of products can vary by country and by state law.

11.2.2 BRAM and VIRP

To help preserve the integrity and goodwill of the payment system, MasterCard has a Business Risk Assessment and Mitigation (BRAM) program, and Visa has an Integrity Risk Program (VIRP) that protects customers against illegal and brand-damaging transactions.

The BRAM and VIRP programmes serve to restrict access to the MasterCard & Visa systems by Merchants whose products and services may pose significant fraud, regulatory, or legal risks. This in turn helps to promote and protect trust in the payment's environment for Cardholders and Merchants alike.

Please see the MasterCard and Visa links below for more information:
Visa Integrity Risk Program (VIRP): Visa Integrity Risk Program
MasterCard Business Risk Assessment & Mitigation Program (BRAM): Mastercard Anti-Piracy Policy

11.3 Terminal Tampering

Keeping your terminal secure is very important. If your terminal is tampered with, this could lead to events such as card or PIN details being copied or stolen by fraudsters. If this happens you will be liable for any losses, you or we suffer due to the fraudster's subsequent actions.

Please check your specific terminals' security policy for further details.

We recommend that you:

- Do not allow any unauthorised access to your EFTPOS terminal.
- Check the terminal regularly for any skimming devices and check the surrounding areas for any cameras.
- Don't disclose your terminal password to anyone, or only tell employee(s) you trust to process refunds. They must keep the password secret.
- Regularly check that all the details on your terminal list still match your EFTPOS terminals.
- Regularly check that stickers haven't been removed, replaced, or damaged.
- Regularly check the cabling to ensure it hasn't been tampered with.
- Check that there are no additional or unknown items of electronic equipment connected to the EFTPOS terminal.

What to do if I suspect anything suspicious?

If you notice anything suspicious, disconnect the terminal immediately and contact Windcave.

Keep the disconnected terminal in a secure place so that evidence such as fingerprints can be preserved.

12 Support and Troubleshooting

12.1 Terminal not working

The most common reasons for your terminal not working are:

- Power failure
- Technical failure with hardware or software
- Telecommunications failure
- Problem with the network switch

Error Message	Description / Action
EFTPOS offline	Host unavailable
Pinpad offline	SCR connection failure
Timeout Declined	Cannot connect to Windcave host
System Fault	Host issuers' fault while authorising card – try a different bank card
Power Failure	Power cut or failure
Unable to process	If consistent this indicates a terminal fault

If the issue is a switch or telecommunications issue, some EFTPOS terminals can perform electronic offline transactions, also known as Electronic Offline Vouchers (EOV). See the EOV section of this guide for more information.

12.2 Cards Failing

Gather as much information as you can so that you can clearly describe what is occurring (is it one type of card, one banks' cards only, or is it cards that have a chip in them etc), then contact Windcave Support

13 American Express

13.1 American Express Merchant Operating Guide

If you have chosen to accept American Express Card using Windcave solutions, you authorise us to submit transactions to, and receive settlement from American Express, on your behalf, and agree to comply with American Express Merchant Operating Guide available here as updated from time to time.

The American Express Merchant Operating Guide sets out the policies and procedures governing your acceptance of the American Express Card. It is part of, and is hereby incorporated by reference into, your Merchant Services Agreement with Windcave. You agree to be bound by and accept all provisions in the American Express Merchant Operating Guide as if fully set out in your Merchant Services Agreement with Windcave and as a condition of your agreement to accept the American Express Card.

13.2 Merchant Information

You hereby give your consent for us to disclose transaction data, merchant data, personal information and other information about you to American Express, its subcontractors and employees.

You agree that American Express collects and retains such information, shares such information with affiliates and its other business lines, and may use information to improve services, operate and promote the American Express Network, prevent fraud, and for other business purposes, including conducting analytics and making information available to certain third-parties, including for tax reconciliation or expense management services and their users.

You agree that American Express may send you commercial marketing messages, including information on products, services, and resources available to your business. You may opt out of receiving American Express commercial marketing communications by contacting us. However, you may continue to receive important transactional or relationship communications from American Express.

13.3 American Express Brand

Whenever payment methods are communicated to customers, or when customers ask what payments are accepted, you must indicate your acceptance of American Express Card and display American Express' Marks as prominently and in the same manner as any other payment products.

You may only use American Express' Marks as permitted under the American Express Merchant Operating Guide and must cease using American Express' Marks upon termination of your Merchant Services Agreement with Windcave.

You must not engage in activities that harm American Express' business or the American Express brand (or both), including by ensuring that your website (if any) does not contain libellous, defamatory, obscene, pornographic or profane material or any other information that may cause harm to any individual or to the American Express brand.

You agree that American Express may enforce the terms of the Merchant Services Agreement between you and Windcave as necessary to protect American Express brand.

13.4 Refund Policies

Your refund policies must be fair and clearly disclosed at the time of sale in compliance with applicable law.

Your refund policy for purchases on the American Express Card must be at least as favourable as your refund policy for purchases made with other payment products or other payment methods.

13.5 Limitation of Liability

You agree that American Express' liability is limited as set out in the American Express Merchant Operating Guide, including but not limited to, American Express' disclaimer relating to data security requirements, warranty of merchantability or fitness for a particular purpose.

13.6 Other

You agree that:

- You will comply with any industry specific requirements of which American Express notifies you in writing from time to time; and
- You will not be able to accept American Express cards if Windcave's agreement with American Express terminates.

14 FAQ's

14.1 General FAQ's

What banks can I use with Windcave?
Windcave in most cases can be your merchant service provider. In the scenario you want to use a different provider, please contact Windcave Support - Windcave | Contact

We (the merchant) process a lot of MOTO transactions; is there a way to streamline this?
Paylink offers a convenient replacement to the MOTO transactions and can be integrated; alternatively, Batch Processor allows you to group all your payments into a spreadsheet (CSV file) to batch process in one go.
Please see our Paylink guide for more information - Windcave | Paylink
Or, view the Batch Processor details here - Windcave | Batch Processor

How do I update my details for my merchant facility?
If you need to change any of your details or information, contact Windcave Support at support@windcave.com

I have a problem with my terminal, who do I contact?
Please contact Windcave Support for any queries in relation to your terminal – support@windcave.com

Where can I find my terminal ID?
Your terminal ID is shown on any transaction receipt.

What happens if I sell my business?
If you sell your business and the new owner wants to retain your terminals, a 'change of ownership' will need to be completed. Please contact your Windcave Sales manager for further information.

I already have a merchant account for my physical store, can I use this for my online business?
An additional electronic merchant number will need to be set up for online payments.

14.2 Hosted Payment Page (HHP)

What is the difference between Merchant Hosted Payment Page (MHPP) and the Hosted Payments Page (HPP)?
The difference is that MHPP takes payment on your secure payment page, and you get the response give back to you in the backend messaging, whereas the Windcave HPP takes payment on the

Windcave secure servers after being forwarded from your site with the order details and we send you back the response to your insecure pages.

14.3 3D Secure Authentication

How does 3D Secure work?

3D secure requires the cardholder to enter a One Time Password (OTP) as an additional step to entering their credit card details that is verified by the issuing bank. Once the issuing bank has verified the code, the user is then re-directed back to the merchants' website and payment is completed.

What Windcave products support 3D Authentication?

3D Authentication is enabled off the shelf with the Hosted Payments Solution (where payment is taken on Windcave's secure pages) and is also available on Merchant Hosted Page session solutions like AJAX or Form POST.

What is 2FA (2-factor authentication)?

2 Factor Authentication (2FA) is an identity and access management security method that requires two forms of identification to access resources and data. 2FA gives businesses the ability to monitor and help safeguard their most vulnerable information and networks.

14.4 Batch Processor

Is the Cardholder name validated?

No, the Cardholder name is not validated – Only the card number and expiry date are verified.

Is there a message I can use to reassure my customers that their transactions will be secure?

The Windcave privacy policy should be linked on your payment page.

14.5 Acquiring

What does Card Present and Card Not Present mean?

Card Present (CP) transactions is when the card used for the purchase is physically in the store at the time of the transaction. All other transactions such as orders taken over the phone, a mail order or online is considered a Card Not Present (CNP) transaction.

14.6 Troubleshooting

My customers are receiving responses that inform that their card type isn't accepted, why is that?

You may not have a merchant facility for a certain card type the customer is trying. Your merchant account with your bank will enable to take Visa and MasterCard payments, If you would like customers to be able to user their Amex and Diners cards (for example), you will need a merchant facility that supports those card types.

15 Document Control Procedure

Document Owner	Acquiring Solutions		
Process Owner	Global Head Acquiring Solutions		
Document Approver	Global Head Acquiring Solutions, Global Head PMO, Risk and Compliance		
Distribution List	Implementations, Acquiring, Compliance		
Audit Date	2023/03/13	**Audit Frequency**	Annually

This document will be reviewed in accordance with the audit frequency but may also be updated to reflect changes as required.